AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (currently amended) A microcircuit card (100) comprising:

a receiver means (RX) for receiving a command (200);

means for modifying at least one characteristic of the performance of said card on reception of said command, the modification means being characterized in that they can be used after a step (E10) of personalization of said card; and

cryptographic means for authenticating the sender of said command,

wherein said receiver means (RX) are configured to receive said command (200) in accordance with an SMS type protocol.

2. (canceled)

3. (previously presented) The microcircuit card according to claim 1, wherein the cryptographic means comprises an authentication key.

4. (previously presented) The microcircuit card according to claim 1, wherein the modification means are adapted to determine said at least one performance characteristic as a function of a predetermined instruction (210) received in said command (200).

5. (canceled)

6. (previously presented) The microcircuit card according to claim 1, wherein said means for modification of at least one performance characteristic are adapted to modify the size of a usable area (110) of a physical memory (EEPROM) of said card.

7. (previously presented) The microcircuit card according to claim 6, wherein said modification of the size of a usable area (110) of a physical memory (EEPROM) is effected by creating, destroying at least one specific file (VOID_FILE) or by modifying the size of at least one specific file (VOID_FILE) comprised in said physical memory.

8. (previously presented) The microcircuit card according to claim 1, wherein said means for modification of at least one performance characteristic are adapted to modify a clock frequency of said card, reversibly or not.

9. (previously presented) The microcircuit card according to claim 1, wherein said means for modification of at least one performance characteristic are adapted to allow or prevent the use of at least one software function (f) of said card, reversibly or not.

10. (previously presented) The microcircuit card according to claim 1, wherein said means for modification of at least one performance characteristic are adapted to allow or prevent the use of all or part of an electronic circuit (120) of said card, reversibly or not.

11. (previously presented) The microcircuit card according to claim 10, wherein said electronic circuit (120) is a cryptographic unit.

12. (previously presented) The microcircuit card according to claim 1, characterized in that it further comprises synchronization means (130) adapted to verify that said command (200) is unique.

13. (currently amended) A method of configuring a microcircuit card (100) comprising the steps of:

personalizing (E10) said card;

receiving (E20) a command (200);

cryptographically authenticating the sender of said command; and

modifying (E40, E60, E70, E80) at least one characteristic of the performance of the card on reception of said command (200),

wherein said receiving step (E20) receives the command in accordance with an SMS type protocol.

14. (canceled)

15. (previously presented) The method according to claim 13, wherein, during said modifying step (E40, E60, E70, E80), said at least one performance characteristic is determined as a function of a predetermined instruction (210) received in said command (200).

16. (canceled)

17. (previously presented) The method according to claim 13, wherein, during said modifying step (E40), the size

of a usable area (110) of a physical memory (EEPROM) of said card is modified.

18. (previously presented) The method according to claim 17, wherein, during said modification of the size of a usable area (110) of a physical memory (EEPROM), at least one specific file (VOID_FILE) included in said physical memory is created, or destroyed or the size of at least one specific file (VOID_FILE) included in said physical memory is modified.

19. (previously presented) The method according to claim 13, wherein, during said modifying step (E60), a clock frequency of said card is modified, reversibly or not.

20. (previously presented) The method according to claim 13, wherein, during said modifying step (E70), the use of at least one software function (f) of said card is allowed or prevented, reversibly or not.

21. (previously presented) The method according to claim 13, wherein, during said modifying step (E80), the use of all or part of an electronic circuit (120) of said card is allowed or prevented, reversibly or not.

22. (currently amended) The method according to claim 21, wherein said electronic ~~component~~ circuit (120) is a cryptographic unit.

23. (previously presented) The method according to claim 13, further comprising the step of:

verifying (E35), prior to said modifying step (E40), that said command (200) is unique.